MODULAR MULTI-MEDIA COMMUNICATION MANAGEMENT SYSTEM

Abstract

The improved AES processing method provides an efficient alternative to both Mips intensive multiplication and to conventional table lookup, used to multiply terms over a Galois field (GF). The improved method takes advantage of the fact that in the GF, any non zero element X can be represented by a power of a primitive element P. The improved method thereby results in a 2 by 256 table. The log base P of the terms being multiplied are looked up and summed, and the anti-log of the sum is looked up in the same table.